

Listing of the Claims

The following listing of claims will replace all prior versions and listings of the claims in the application:

1. (Currently Amended) A crypto algorithm unit comprising:
a first crypto hash execution module; and
a second crypto hash execution module, wherein the first crypto execution module and the second crypto execution module share a plurality of components to form a combination crypto algorithm unit, wherein the ~~plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution~~ combination crypto algorithm unit being capable of performing an MD5 hash algorithm and a SHA1 hash algorithm, the combination crypto algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm;
and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm.

2. (Original) The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes a plurality of muxes.

3. (Original) The crypto algorithm unit of claim 2, wherein the plurality of muxes provides a crypto hash algorithm selection control.

4. (Original) The crypto algorithm unit of claim 3, wherein the crypto hash algorithm selection control allows the selection of a first subset of the plurality of components, wherein the selected first subset of the plurality of components can execute a first crypto algorithm.

5. (Canceled)

6. (Canceled)

7. (Currently Amended) The crypto algorithm unit of ~~claim 1~~claim 6, wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of ~~an MD5 hash algorithm, a~~ the SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution module is capable of executing.

8. (Original) The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit is on a single integrated circuit die.

9. (Original) The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit and a microprocessor are on a single integrated circuit die.

10. (Original) The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes one or more full adders.

11. (Canceled)

12. (Currently Amended) The crypto algorithm unit of claim 1, wherein the combination crypto algorithm unit includes ~~one or more~~ a plurality of compressors.

13. (Canceled)

14. (Currently Amended) An integrated circuit comprising:

a microprocessor core; and

a combination crypto algorithm unit, the combination crypto algorithm unit being coupled to the microprocessor core wherein the combination crypto algorithm unit includes a first crypto execution module and a second crypto hash execution module, wherein the first crypto execution module and the second crypto execution module share a plurality of components, wherein the ~~plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution~~ combination crypto algorithm unit being capable of performing an MD5 hash algorithm and a SHA1 hash algorithm, the combination crypto algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm;

and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Currently Amended) The integrated circuit of ~~claim 14~~claim 17, wherein the second crypto hash execution module is capable of executing at least one of a group of crypto hash algorithms consisting of ~~an MD5 hash algorithm, a~~ the SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the crypto hash algorithm that the first crypto hash execution module is capable of executing.

19. (Currently Amended) A method of executing a crypto instruction comprising:

receiving a first crypto hash instruction in a combination crypto algorithm unit;

determining a corresponding first crypto hash algorithm for the first crypto instruction;

selecting a first plurality of components in the combination crypto algorithm unit including a first crypto execution module and a second crypto hash execution module, wherein the first crypto execution module and the second crypto execution module share a plurality of components, wherein the ~~plurality of shared components include one or more adders, wherein each one of the one or more shared adders are included in the first crypto hash execution module and used to perform the first crypto hash execution and wherein each one of the one or more shared adders are included in the second crypto hash execution module and used to perform the second crypto hash execution~~ combination crypto algorithm unit being capable of performing an MD5 hash algorithm and a SHA1 hash algorithm, the combination crypto algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm;
and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm;
and

executing the first crypto hash instruction through the selected first plurality of components.

20. (Original) The method of claim 19, further comprising:

receiving a second crypto hash instruction in the combination crypto algorithm unit;

determining a corresponding second crypto hash algorithm for the second crypto hash instruction;

selecting a second plurality of components in the combination crypto algorithm unit; and

executing the second crypto hash instruction through the selected second plurality of components, the selected second plurality of components and the selected first plurality of components sharing a third plurality of components.